



PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2003069644 A

(43) Date of publication of application: 07.03.2003

(51) Int. Cl. H04L 12/56

G06F 13/00, H04M 3/00

(21) Application number: 2001258398

(22) Date of filing: 28.08.2001

(71) Applicant: TOSHIBA CORP

(72) Inventor: WATANABE MASANORI

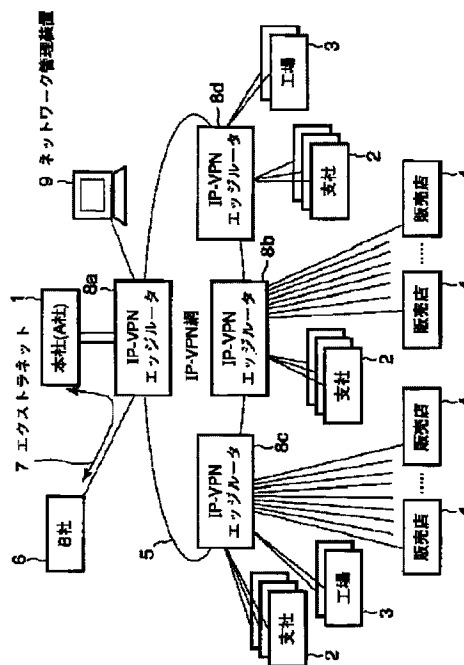
(54) NETWORK MANAGEMENT DEVICE

COPYRIGHT: (C)2003,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To realize a service which monitors the present network operation state to predict the future tendency and presents it to clients.

SOLUTION: A network management device 9 connected to an IP-VPN (virtual private network) network 5 constructed as an enterprise network is provided with a function which periodically collects information required for quality management like a transmission/reception traffic volume from an edge router set as a management object out of IP-VPN edge routers 8a, 8b, 8c and 8d of the IP-VPN network 5 and predicts the tendency of the future operation condition like transition of future traffic and reports the prediction result. Thus, smooth network extension and update or change of service like QoS (quality of service) can be proposed to clients to prevent a lack of bands and the degradation in quality in the future.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-69644

(P2003-69644A)

(43)公開日 平成15年3月7日(2003.3.7)

| (51)Int.Cl. ⁷ | 識別記号 | F I | テーマコード [*] (参考) |
|--------------------------|-------|---------------|--------------------------|
| H 0 4 L 12/56 | 4 0 0 | H 0 4 L 12/56 | 4 0 0 B 5 B 0 8 9 |
| G 0 6 F 13/00 | 3 5 3 | G 0 6 F 13/00 | 3 5 3 B 5 K 0 3 0 |
| H 0 4 M 3/00 | | H 0 4 M 3/00 | D 5 K 0 5 1 |

審査請求 未請求 請求項の数7 O L (全 9 頁)

(21)出願番号 特願2001-258398(P2001-258398)

(22)出願日 平成13年8月28日(2001.8.28)

(71)出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72)発明者 渡辺 正徳

東京都府中市東芝町1番地 株式会社東芝

府中事業所内

(74)代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム(参考) 5B089 JA35 JB14 KA13

5K030 GA14 HA08 HB11 HC01 HC13

HD03 JA10 JL07 KA05 MA01

MA04 MB02 MB09 MC07 MC08

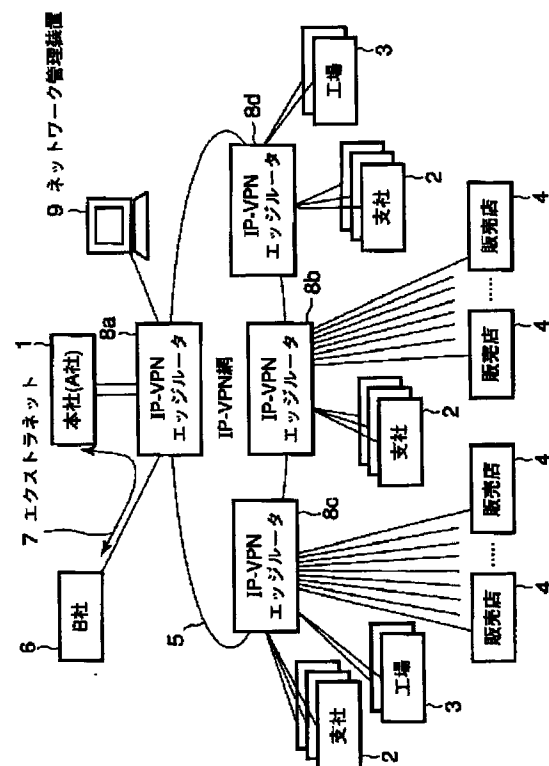
5K051 CC08 DD03 FF01 FF03

(54)【発明の名称】 ネットワーク管理装置

(57)【要約】

【課題】現在のネットワーク運用状態を監視して今後の動向を予測して顧客に提示するサービスを実現する。

【解決手段】企業網として構築されたIP-VPN網5のIP-VPNエッジルータ8a、8b、8c、8dの中で管理対象として設定されたエッジルータから送受信トラフィック量などの品質管理に必要な情報を定期的に収集し、将来のトラフィックの推移など今後の運用状況の動向を予測し、その予測結果を通知する機能をIP-VPN網5に接続されたネットワーク管理装置9に備える。これにより、顧客に対してスムーズなネットワークの拡張やQoSなどのサービスの更新、変更を提案でき、将来の帯域不足や品質低下を未然に防ぐことができる。



【特許請求の範囲】

【請求項1】 企業網として各拠点間を結ぶ特定のネットワークに接続されて、上記ネットワークの運用状態を監視するネットワーク管理装置であって、

上記各拠点と上記ネットワークとの間に介在して上記企業に関するデータを論理的に他のデータと分離してルーティング処理する各ルータのうち、管理対象として設定されたルータから品質管理に必要な情報を定期的に収集する情報収集手段と、

この情報収集手段により収集された情報を解析して今後のネットワーク運用状態の動向を予測する予測手段と、この予測手段によって予測された結果を通知する通知手段とを具備したことを特徴とするネットワーク管理装置。

【請求項2】 企業網として各拠点間を結ぶ特定のネットワークに接続されて、上記ネットワークの運用状態を監視するネットワーク管理装置であって、

上記各拠点と上記ネットワークとの間に介在して上記企業に関するデータを論理的に他のデータと分離してルーティング処理する各ルータのうち、管理対象として設定されたルータから少なくとも送受信トラフィック量を定期的に収集する情報収集手段と、

この情報収集手段により収集された送受信トラフィック量を解析して今後のトラフィック量の増減を予測する予測手段と、

この予測手段によって予測された結果を通知する通知手段とを具備したことを特徴とするネットワーク管理装置。

【請求項3】 上記通知手段は、上記予測手段により契約時に保証されたトラフィック量を超過すると判定された場合にその旨を通知することを特徴とする請求項2記載のネットワーク管理装置。

【請求項4】 企業網として各拠点間を結ぶ特定のネットワークに接続されて、上記ネットワークの運用状態を監視するネットワーク管理装置であって、

上記各拠点と上記ネットワークとの間に介在して上記企業に関するデータを論理的に他のデータと分離してルーティング処理する各ルータのうち、管理対象として設定されたルータから品質サービスを利用している送信元アドレスと送信先アドレスのペア数、それらの送受信トラフィック量を定期的に収集する情報収集手段と、

この情報収集手段により収集された送信元アドレスと送信先アドレスのペア数、送受信トラフィック量を解析して今後のサービス利用状況を予測する予測手段と、

この予測手段により予測された結果を通知する通知手段とを具備したことを特徴とするネットワーク管理装置。

【請求項5】 上記通知手段は、上記予測手段により契約時に保証されたサービス品質を低下すると判定された場合にその旨を通知することを特徴とする請求項4記載のネットワーク管理装置。

【請求項6】 企業網として各拠点間を結ぶ特定のネットワークに接続されて、上記ネットワークの運用状態を監視するネットワーク管理装置であって、

上記各拠点と上記ネットワークとの間に介在して上記企業に関するデータを論理的に他のデータと分離してルーティング処理する各ルータのうち、管理対象として設定されたルータから品質サービスの各クラス毎の送受信トラフィック量、各クラスでのポート番号毎の送受信トラフィック量を定期的に収集する情報収集手段と、

この情報収集手段により収集された各クラス毎の送受信トラフィック量、各クラスでのポート番号毎の送受信トラフィック量を解析して、今後のサービス利用状況を各クラス別に予測する予測手段と、

この予測手段によって予測された結果を通知する通知手段とを具備したことを特徴とするネットワーク管理装置。

【請求項7】 上記通知手段は、上記予測手段により契約時に保証されたサービス品質を低下するクラスがあると判定された場合にその旨を通知することを特徴とする請求項6記載のネットワーク管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、企業の拠点間を結ぶネットワークの運用状態を管理するネットワーク管理装置に関する。

【0002】

【従来の技術】従来の企業ネットワークは、求められる品質、安定度の高さ、さらにセキュリティの観点から専用線を使用したネットワーク構築が一般的であった。しかし、インターネットの普及、インターネットのバックボーンの帯域、品質の進歩、インターネット上で仮想的に企業網（VPN：Virtual Private Network）を構築する技術の確立により、多くの企業が自社の広域ネットワークをインターネット上に構築しようとしている。これにより、企業網の中、遠距離の転送に要するコストを大幅に削減することが可能になり、通信事業者が提供するアウトソーシングサービスを利用すれば、更なるコストの削減が図れることから今後も多くの企業がVPNの導入を進める傾向にある。

【0003】この通信事業者が提供するVPNには、暗号化によりセキュリティを考慮したインターネットVPNと呼ばれるものや、暗号化によるセキュリティだけではなく、インターネット上を転送される他のトラフィックと論理的に分離することによって、より高いセキュリティを提供し、さらに専用線のような高い品質を実現するIP-VPNなどがある。

【0004】IP-VPNとは、通信事業者の閉域IPネットワーク網を通信経路として用いる仮想専用網のことであり、複数のプロバイダのネットワークを経由する必要があるインターネットを用いないため、エンド・ト

ウ・エンドで機密性や通信品質に優れたIP接続が行える。

【0005】ここで、IP-VPNサービスでは、帯域や品質、セキュリティなど、顧客の多様な要求に対応すべく様々なオプションが用意されており、これらをどのように選択するかは、各企業にあったネットワークの設計によって決定される。企業が企業網の一新、もしくは変更を行うなど、新たなネットワークを設計する上でもっとも必要となるのは、現状のネットワークの運用状態の調査とその解析、今後のトラヒックの予測であり、それらを基にその帯域や品質（トラヒック量や転送レートなど）を決定する。これらの情報が正確であればあるほど、新ネットワークに移行した後の安定的な運用が保証され、トラブルの発生を抑えることができる。

【0006】しかし、ネットワークに接続する端末、拠点の増加とともにそのネットワーク設計が複雑化しており、ネットワークの運用状態の調査、解析、将来のトラヒックの予測は困難で、正確に行おうとすれば多くの時間と費用を要することになる。また、ネットワーク全般の技術革新も著しく、その調査、解析および予測に時間を掛けすぎると、次から次へと出てくる新たなサービスに対応できなくなってしまう。かといって、不十分な調査結果、予測でネットワークを設計してしまうと、導入後のトラブル等で再度詳細な調査、解析が必要となり、多大な損失を生んでしまう。

【0007】また、近年のネットワーク技術者の慢性的な不足などにより、企業網の自営が困難となっており、通信事業者のアウトソーシングサービスを選択する企業が現れており、今後この流れは加速するものと予測される。アウトソーシングサービスを提供する通信事業者としても、運用状態の正確な調査、解析、将来のトラヒックの増加の予測は、将来のトラブルを回避するために必須ではあるが、ある程度の運用状態の監視は行っているものの、常に将来のトラヒックを念頭においての運用監視は行えていないのが現状である。

【0008】

【発明が解決しようとする課題】上述したように、従来、企業網を新規もしくは変更する時点で、企業は独自に、もしくは通信事業者やコンサルティング会社等に依頼して現状の運用状態を監視することはあるが、それは単にトラブルが発生していないかという観点からの監視であって、将来のネットワークを設計する上で参考となる情報を収集しているものではない。

【0009】なお、ネットワークの品質を管理するものとして、特開2001-69170号公報の「品質予測値提示通信網」が知られている。しかしながら、上記公報では、品質が保証されていないオープンなネットワークを前提とし、ルータ間のリンクのトラヒック情報に基づいて遅延や損失の少ないデータの転送経路（ルート）を検証するものであって、上述したIP-VPNのよう

に品質が保証された閉域ネットワークによって構築された企業網を対象として、現在のネットワーク運用状態を監視することはできない。

【0010】そこで、本発明は、品質が保証されたネットワークにより企業網が構築されている場合において、現在のネットワーク運用状態を監視して今後の動向を予測して顧客に提示するサービスを実現するネットワーク管理装置を提供することを目的とする。

【0011】

10 【課題を解決するための手段】本発明のネットワーク管理装置は、企業網として各拠点間を結ぶ特定のネットワークに接続されて、上記ネットワークの運用状態を監視するネットワーク管理装置であって、上記拠点と上記ネットワークとの間に介在して上記企業に関するデータを論理的に他のデータと分離してルーティング処理する各ルータのうち、管理対象として設定されたルータから品質管理に必要な情報を定期的に収集する情報収集手段と、この情報収集手段により収集された情報を解析して今後のネットワーク運用状態の動向を予測する予測手段と、この予測手段によって予測された結果を通知する通知手段とを具備して構成される。

20 【0012】このような構成のネットワーク管理装置によれば、企業網を構成するネットワーク上の各ルータの中で管理対象として設定されたルータから品質管理に必要な情報が本装置によって定期的に収集される。上記品質管理に必要な情報とは、例えば当該ルータにおける送受信トラヒック量である。このようにして収集された情報から今後のネットワーク運用状態の動向が予測されて通知される。すなわち、例えば現在のトラヒック量から今後のトラヒック量の増減が予測されて、契約時に保証されたトラヒック量を超過するような場合にその旨が通知される。したがって、管理者はその通知を受けることで、顧客にネットワークの拡張などを提案でき、将来の帯域不足や品質低下のトラブルを未然に防ぐことができると共に、顧客側では企業網の運用状態がより正確に把握できるため、スムーズな契約の更改を行うことができる。

【0013】

40 【発明の実施の形態】以下、図面を参照して本発明の一実施形態を説明する。

【0014】図1は本発明の一実施形態に係るネットワーク構成を示す図であり、IP-VPNサービスを使用したA社の企業網の一例が示されている。

【0015】図1において、A社は、本社1と、全国に点在する多数の支社2、工場3および販売店4などを結んで企業網としてのIP-VPN網5を構築している。また、IP-VPN網5内のNAT（Network Address Translator）を利用して提携会社であるB社とのエクストラネット7も構築している。

50 【0016】通信事業者が提供するIP-VPNサービ

スは、インターネット上に論理的に切り離されたネットワークを構築し、それを企業網の中、長距離のデータ転送路とする。図1では、IP-VPNエッジルータ8a、8b、8c、8d間がこれに当たる。これらのIP-VPNエッジルータ8a、8b、8c、8dは、キャリア側のネットワークと顧客側のネットワークとの間に介在し、特にIP-VPNでは暗号化やトンネリングなどによって他のデータと論理的に分離してルーティング処理を行う機能を有する。

【0017】IP-VPN網5で結ばれた本社1、支社2、工場3、販売店4の各拠点は、それぞれに対応したIP-VPNエッジルータ8a、8b、8c、8dに接続されており、例えば高速デジタル回線(HSD: High Super Digital)、ATM(Asynchronous Transfer Mode)専用線、FR(Frame Relay)回線、ISDN(Integrated Services Digital Network)回線などを利用してIP-VPN網5にアクセスする。

【0018】また、このIP-VPN網5には、IP-VPNエッジルータ8aを介して本発明のネットワーク管理装置9が接続されている。このネットワーク管理装置9は、IP-VPN網5に設けられた各IP-VPNエッジルータ8a、8b、8c、8dから定期的に品質管理に必要な情報を収集して蓄積し、その収集、蓄積された情報を分析して今後の運用状態の動向を予測する機能を備える。

【0019】このような構成において、A社の企業網の運用状態を調査する場合には、その企業網を構成するIP-VPNエッジルータ8a、8b、8c、8dの動作状態を管理することが重要となる。なお、IP-VPNエッジルータ8a、8b、8c、8d間には、IP-VPNサービスの基幹となるバックボーンに図示せぬIP-VPNコアルータが多数存在している。このIP-VPNコアルータはIP-VPNエッジルータ8で集約されたデータを転送するものであり、別の顧客からのデータも含まれる。したがって、そこでの情報からはA社の企業網に関する運用状態を解析するには精度の粗いものとなるため、ここではIP-VPNコアルータは管理対象外としている。

【0020】一般的に本社1、支社2、工場4などは頻繁に増減するものではないが、販売店4ともなると頻繁にその数が増減することが考えられる。また、経理システムなどのアプリケーションを新しいものに変更する場合には、全社一斉に変更するケースが多く、アプリケーション自体が一斉に変更されるため、転送されるパケットの品質も激変することも考えられる。

【0021】このようなことを考慮すると、A社の企業網の運用状態の調査では、IP-VPNエッジルータ8a、8b、8c、8dから以下のような項目に関する情報を定期的に収集する必要がある。

【0022】・Upstream(アクセス側からバ

ックボーン側)のトラフィック量

・Downstream(バックボーン側からアクセス側)のトラフィック量

・アクセス側のルーティングキャッシュの送信元アドレス数

・アクセス側のルーティングキャッシュの送信先アドレス数

・バックボーン側のルーティングキャッシュの送信元アドレス数

・バックボーン側のルーティングキャッシュの送信先アドレス数

・アプリケーション毎のUpstreamの送受信トラフィック量

・アプリケーション毎のDownstreamの送受信トラフィック量

・各品質レベル毎のUpstreamの送受信トラフィック量および廃棄トラフィック量

・各品質レベル毎のDownstreamの送受信トラフィック量および廃棄トラフィック量

・IP-VPN網内の各種NATとの送受信トラフィック量などである。

【0023】これらの情報を定期的に収集して解析することにより、企業網全体の現状の運用状態を把握でき、その時間的推移を検証することにより、将来のトラフィックの推移など今後の運用状態の動向を予測することが可能となる。

【0024】すなわち、例えば、アクセス側の端末数やどのアプリケーションのデータ転送が増加しているのか、NATを使っているインターネットアクセスがどの程度増加しているのか、エクストラネットでのデータ転送がどのくらい増えているのかなど、そのネットワークの変動状況が判明する。これらの情報の収集、解析、予測は図1のネットワーク管理装置9にて行われる。

【0025】ネットワーク管理装置9には、SNMP(Simple Network Management Protocol)といったネットワーク管理プロトコルが使用されている。SNMPは、TCP/IPネットワークでネットワーク管理システムを構成するためのプロトコルであり、ネットワークに接続されたルータやブリッジなどの各種管理対象となるネットワーク構成機器(エージェントと呼ばれる)から管理に必要な情報を授受する方法が規定されている。

【0026】図1の例では、IP-VPNエッジルータ8a、8b、8c、8dの中で管理対象として設定された任意のIP-VPNエッジルータから収集した所定の情報を元に、例えば1ヵ月後、3ヵ月後、半年後、1年後といったように、将来の企業網の運用状態の予測を行うシステムがネットワーク管理装置9に搭載されており、それをスムーズなネットワークの拡張、新規ネットワークの設計に役立たせるものである。

【0027】以下に、具体例を挙げて説明する。

【0028】例えば、図2に示すように、IP-VPNエッジルータ8bに接続された支店2や販売店4からIP-VPN網5を介してIP-VPNエッジルータ8aに接続された本社1の顧客登録サーバ10へアクセスする場合において、高い品質での通信を保証するQoS (Quality of service) サービスを利用しているケースを考える。QoSとは、ネットワークのサービス品質のことであり、OSI参照モデルではネットワーク層(第3層)で規定されており、例えば音声や動画などの一定の帯域が必要なアプリケーションやリアルタイム性を要求する通信に優先的に帯域を割り当てるなどの制御を行う。

【0029】A社は、本社1と全支店2、全販売店4で使用する顧客登録のアプリケーションの使用頻度が高く、高いレスポンスを要求することから、これらに関するデータの転送に対し、優先度の高いトラヒックの帯域を優先的に確保、転送するQoSサービスを5Mbpsの帯域だけ契約しているものとする。図2に示すIP-VPNエッジルータ8a、8b(ルータAとルータB)には、このQoSサービスを利用するトラヒックを他のトラヒックと分離するために、その送信元アドレスと送信先アドレスが登録されている。そして、IP-VPNエッジルータ8bが支店2から本社1へのデータを受信した際に、その受信したデータの送信元アドレスと送信先アドレスがQoSサービス用として予め登録された送信元アドレスと送信先アドレスに該当するかどうかをチェックする。そして、QoSサービスに該当する場合には、そのデータにQoSの高いデータを示すフラグを付けてIP-VPNエッジルータ8aへ転送する。それを受信したIP-VPNエッジルータ8aは、上記フラグに基づいて当該データを優先的に本社1の顧客登録サーバ10に転送する。本社1から支店2へのデータ転送時についても同様である。

【0030】<ケース1>ここで、上記図2のようなケースでは、QoSサービスの利用によるデータの転送状態を監視するためには、ネットワーク管理装置9では、本社1に接続されたIP-VPNエッジルータ8aから以下のような情報を収集する。

【0031】・QoSサービスを利用している送信元アドレスと送信先アドレスのペアの数

・QoSサービスを利用している各通信の送受信トラヒック量

これらの情報を定期的に収集した結果、ネットワーク管理装置9には、図3に示すような情報が蓄積される。図3の例では、2001年1月21日～同年4月21日までの3ヶ月間に亘って一定時間間隔(30分間隔)でIP-VPNエッジルータ8aから情報を収集した場合のQoS利用数、QoS利用時の送信トラヒック量と受信トラヒック量との関係が示されている。

【0032】この情報収集結果から現状のQoSサービスの利用状況を具体的に把握することが可能になり、QoSサービスを利用するクライアントの台数の推移とそのトラヒック量の推移から以下のようなことを解析できる。

【0033】(1)2001.1.21から2001.4.21の3ヶ月間で、QoSサービスを利用しているクライアントの数が最大71から83に増加している。

(2)2001.1.21から2001.4.21の3ヶ月間で、QoSサービスを利用しているクライアントからサーバ方向のトラヒック量が平均1.0031倍に増加している。

(3)2001.1.21から2001.4.21の3ヶ月間で、QoSサービスを利用しているサーバからクライアント方向のトラヒック量が平均1.0032倍に増加している。

【0034】以上のような解析結果から、例えば2ヶ月後の2001.8.4には、QoSサービスを利用するトラヒックのうち、クライアントからサーバ方向のトラヒックが契約時の5Mbpsを超える可能性が高くなることなどを予測することができる。

【0035】このように、ネットワーク管理装置9はIP-VPNエッジルータ8aから収集した情報に基づいて、回帰計算などの所定の予測計算式を用いて今後の運用状態を予測する。その際、図4に示すようなトラヒック予測図を作成して、契約している帯域の超過や品質がSLA(Service Level Agreement: サービス品質保証契約)よりも低下することなどを予測した場合に、通信事業者の管理担当者に通知する。

【0036】通知方法としては、特に限定されるものではないが、例えばネットワーク管理装置9に備えられているモニターに上記図4のトラヒック予測図を表示すると共に、将来、SLAより低下することが予測される場合にその旨をメッセージ表示するなどの方法がある。これを受けて、通信事業者は、顧客に対し、ネットワークの拡張や、新たなサービス内容の契約、変更を提案することで、帯域超過や品質の低下を未然に防ぐことができる。

【0037】なお、図2の例では、本社1に対するアクセスを監視するためにIP-VPNエッジルータ8aを情報を収集するものとしたが、IP-VPNエッジルータ8bや他のIP-VPNエッジルータに接続された支店2や販売店4などに対するアクセスを監視する場合には、上記同様にして、そこでのIP-VPNエッジルータの情報を収集することで実現できる。どのルータを管理対象とするのかは管理項目に応じて決定される。ネットワーク管理装置9にはその管理対象として設定されたルータの位置情報が登録されており、IP-VPNエッジルータ8aを起点にして当該ルータの情報を収集することになる。

【0038】<ケース2>次に、図5に示すように、A社の本社1と支社2との間に低、中、高の3つのQoSのサービスクラスの帯域が契約されている場合を想定する。低クラスの帯域は5Mbps、中クラスの帯域は10Mbps、高クラスの帯域は20Mbpsであり、これらのクラスはアプリケーションに応じて使い分けされている。アプリケーションとは、例えば経理システムなどであり、複数のアプリケーションを使用する場合には、各アプリケーションの使用頻度、重要度などに応じて図5のようにサービスクラスを分けることがある。

【0039】ここで、ネットワーク管理装置9から以下のような情報をIP-VPNエッジルータ8aから収集する。

【0040】・複数のサービスクラス毎の送受信トラフィック量

・各サービスクラスでTCP/UDPポート番号毎の送受信トラフィック量

ネットワーク管理装置9はこれらの情報を定期的に収集、蓄積することで、現状のQoSサービスの利用状況を分析し、各サービスクラス毎にアプリケーションの推移とそのトラフィック量の推移から以下のような分析を行う。

【0041】(1)2001.1.21から2001.4.21の3ヶ月間で、QoSサービス：高を利用して支社2から本社1向けのトラフィックが最大4.3Mbpsから2.1Mbpsに減少している。

(2)2001.1.21から2001.4.21の3ヶ月間で、QoSサービス：中を利用して支社2から本社1向けのトラフィックが最大6Mbpsから8.7Mbpsに増加している。

(3)2001.1.21から2001.4.21の3ヶ月間で、TCP・Port・Number：6539の通信が1日平均1.021倍で増加している。

【0042】以上のような分析結果から、例えば45日後の2001.6.5には、QoSサービス：中を利用するトラフィックのうち、支社2から本社8向けのトラフィックが契約している10Mbpsを超える可能性が高いと予測できる。

【0043】また、既にQoSサービスクラス：高を利用してトラフィックが契約の5Mbpsの50%に到達することはなく、15日後には契約帯域を2Mbpsにしても十分運用可能であると予測できる。

【0044】ネットワーク管理装置1は、このような予測の結果から現在の契約されている帯域の超過などを予測した場合に、通信事業者の管理担当者にその旨を通知する。

【0045】上記ケース1、2のように、予測したいトラフィック量、品質に合わせて、測定するポイント、測定項目を選び、それらをネットワーク管理装置9で収集、蓄積、分析して予想を行うことで、将来のトラブルを未

然に防ぐことができ、かつ、顧客の満足度の高いサービスを提供することが可能となる。

【0046】また、上記ケース1、2以外には、以下のような例が考えられる。

【0047】・IP-VPNエッジルータ8a、8b、8c、8dのそれぞれが転送しているトラフィック量を定期的に測定することにより、エッジルータ自身の転送能力の限界に達する時期を予測し、事前に、より転送能力の高い機器への変更を推奨する。

10 【0048】・IP-VPNエッジルータ8a、8b、8c、8dにおけるOSPF (OpenShortest path first) 等のダイナミックルーティングプロトコルの情報パケットのロスなどを定期的に測定することにより、ルーティング情報の処理限界に達する時期を予測し、事前に、より処理能力の高い機器への変更、ルーティングのデザインの変更を推奨する。

【0049】・NATを経由するトラフィック量を定期的に測定することにより、現在使用中のNATのアドレス変換能力の限界に達する時期を予測し、事前に、より変換能力の高い機器への変更を推奨する。

20 【0050】図6に上記の機能を実現するネットワーク管理装置9の処理の概要を示す。

【0051】ネットワーク管理装置9は、情報収集機能部21、情報蓄積部22、トラフィック予測機能部23、運用状態表示部24を備えている。なお、このネットワーク管理装置9は、例えば磁気ディスク等の記録媒体に記録されたプログラムを読み込み、このプログラムによって動作が制御されるコンピュータによって実現される。

30 【0052】統計情報収集機能部21は、SNMP等のネットワーク管理プロトコルを使用して、IP-VPN網5上の管理対象装置20から各種情報を定期的に収集する。上記管理対象装置20とは、図1のIP-VPN網5を構成する各IP-VPNエッジルータ8a、8b、8c、8dの中で管理対象として設定されたIP-VPNエッジルータのことである。収集情報蓄積部22は、情報収集機能部21にて収集された情報を蓄積する。

40 【0053】トラフィック予測機能部23は、情報蓄積部22に蓄積された情報を解析し、所定の計算式を用いて今後のトラフィックを予測し、その結果を情報蓄積部22に送って蓄積する。このとき、予測されたトラフィックが契約時のトラフィックを越えるような場合に、トラフィック予測機能部23はその旨を運用状態表示部24を通じて管理者に通知する。

50 【0054】管理者はその通知を受けると、予測されたトラフィックの情報を元にして帯域の拡張やQoSなどの各種オプションの変更などを顧客に提案する。これにより、将来のトラブルを未然に防ぐことができると共に、通信事業者は契約内容の更新を効率的に行うことが可能

となる。また、このような予測結果を定期的に顧客に情報提供すれば、顧客側では自社の企業網の運用状態がより正確に把握できるため、スムーズな契約の更改を行うことができるようになる。

【0055】

【発明の効果】以上詳記したように本発明によれば、品質が保証されたIP-VPNなどの特定のネットワークにより構築された企業網において、ネットワーク上の管理対象として設定されたルータから品質管理に必要な情報を定期的に収集し、将来のトラヒックの推移など今後の運用状況の動向を予測し、その予測結果を通知する機能を同ネットワークに接続されたネットワーク管理装置に備えることで、顧客に対してスムーズなネットワークの拡張やQoSなどのサービスの更新、変更を提案できる。これにより、将来の帯域不足や品質低下を未然に防ぐことが可能となり、通信事業者は予測結果を顧客に提供するサービスを行うことで、ネットワーク事業をさらに向上させることができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るネットワーク構成を示す図であり、IP-VPNサービスを使用した企業網の一例を示す図。

【図2】QoSサービスを利用している企業網の一例を*

*示す図。

【図3】QoSサービス利用状況の情報収集結果を示す図。

【図4】情報収集結果に基づいて作成されたトラヒック予測図。

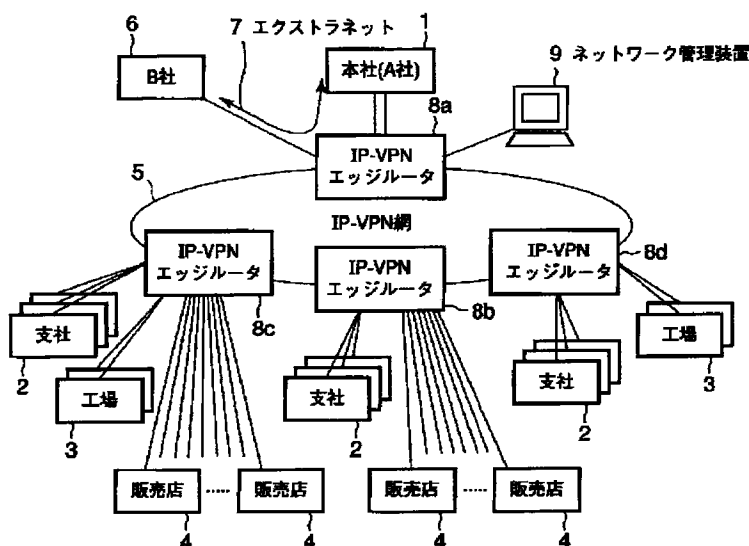
【図5】複数のクラス別にQoSサービスを利用している企業網の一例を示す図。

【図6】本発明のネットワーク管理装置の処理機能を示すブロック図。

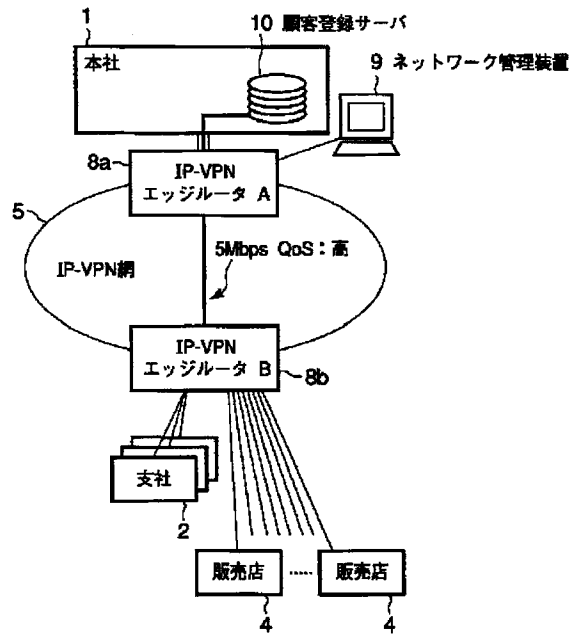
【符号の説明】

- 1～4…A社の拠点
- 5…IP-VPN網（A社の企業網）
- 6…B社
- 7…エクストラネット
- 8a～8d…IP-VPNエッジルータ
- 9…ネットワーク管理装置
- 10…顧客登録サーバ
- 20…管理対象装置（IP-VPNエッジルータ）
- 21…情報収集機能部
- 22…情報蓄積部
- 23…トラヒック予測機能部
- 24…運用状態表示部

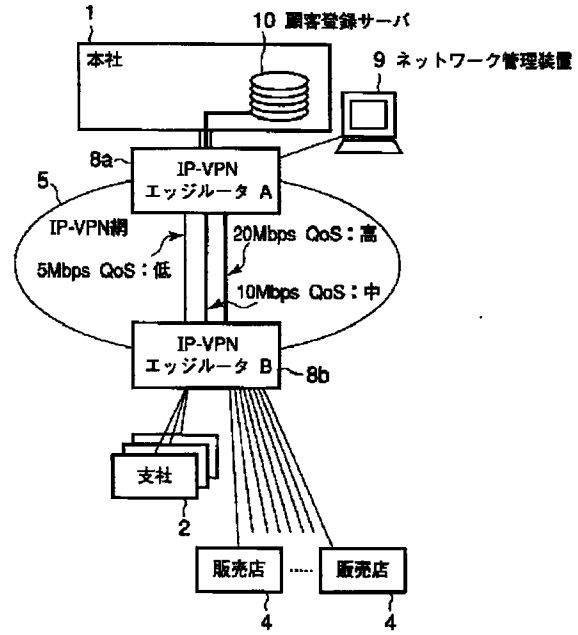
【図1】



【図2】



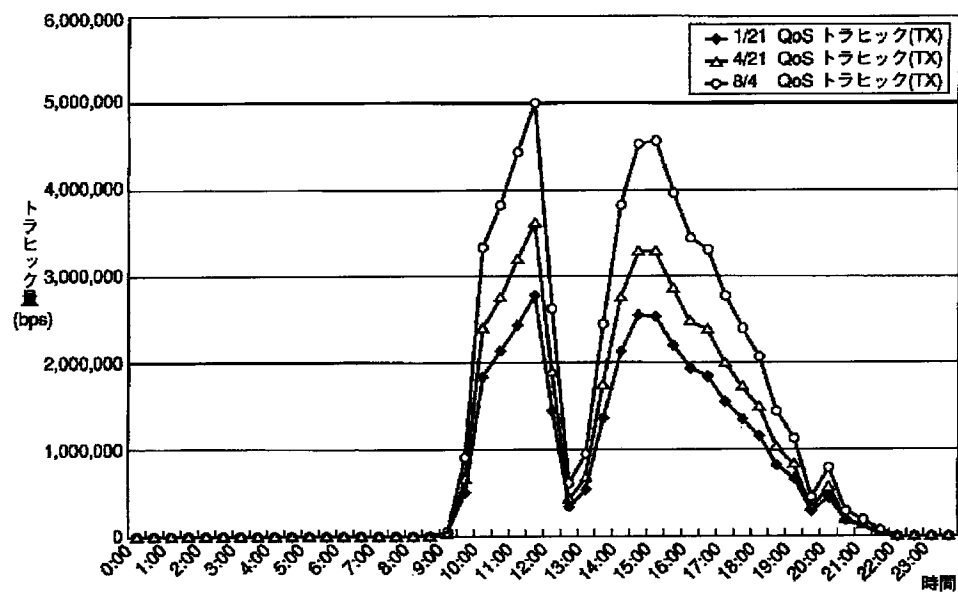
【図5】



【図3】

| Date | Time | QoS利用数 | QoS利用トラヒック量(送信) | QoS利用トラヒック量(受信) |
|-----------|-------|--------|-----------------|-----------------|
| 2001.1.21 | 10:00 | 58 | 1.843 Mbps | 1.233 Mbps |
| | 10:30 | 62 | 2.122 Mbps | 1.443 Mbps |
| | 11:00 | 66 | 2.431 Mbps | 1.562 Mbps |
| | 11:30 | 71 | 2.782 Mbps | 1.873 Mbps |
| | 12:00 | 41 | 1.440 Mbps | 0.958 Mbps |
| | 12:30 | 8 | 0.328 Mbps | 0.253 Mbps |
| | 13:00 | 15 | 0.525 Mbps | 0.588 Mbps |
| ⋮ | | | | |
| 2001.4.21 | 10:00 | 70 | 2.884 Mbps | 2.042 Mbps |
| | 10:30 | 74 | 3.211 Mbps | 2.235 Mbps |
| | 11:00 | 78 | 3.443 Mbps | 2.433 Mbps |
| | 11:30 | 83 | 3.611 Mbps | 2.638 Mbps |
| | 12:00 | 52 | 2.002 Mbps | 1.433 Mbps |
| | 12:30 | 11 | 0.503 Mbps | 0.327 Mbps |
| | 13:00 | 23 | 0.944 Mbps | 0.766 Mbps |

【図4】



【図6】

